Web Application Security Assessment Q&A
Public Employees Retirement Association of Minnesota
April 20, 2012

Q1: How many applications/web sites are in scope?
A1: Four unique web sites are in scope. Although we have one large integrated application, each website hits a separate section of the application.

Q2: What can you tell me about the applications?
A2: Our applications are custom applications written in Delphi. The two main applications, CAMI and ERIS, are accessed off our website, www.mnpera.org. More information will be provided at a private meeting between PERA and the firm that wins this contract.

Q3: Will this be unauthenticated or authenticated testing or both?
A3: Both. The vendor will first be asked to use "black" tests to attempt to gain access to our systems, then will be provided with credentials to access systems as a member and as an employer to see if the user is able to access data that should not be available to that member and employer.

Q4: Will testing be done on a replicated test environment or in a production environment?
A4: Testing will be done in a production environment.

Q5: Do you have a CVS tool in the environment?
A5: No.

Q6: Are applications hosted by a 3rd party?
A6: No. They are hosted onsite.

Q7: Are applications made up of web-input forms, web-services or flash components?
A7: Web-input forms.

Q8: Is a brute force attack allowed to gain credentialed access?
A8: Specific tests will be discussed with the vendor, but brute force attacks will likely be allowed.

Q9: Is susceptibility to denial of service attacks in scope?
A9: Again, specific tests will be discussed with the vendor, but denial of service attacks will likely be in scope.

Q10: Is there a limit on the duration the application can be assessed on a daily basis?
A10: There may be limits, depending on how disruptive the tests will be on our systems. The vendor will be attempting to "hack" our production environment while it is being accessed by staff,

members and employers. When we meet with the vendor we will determine when tests should be run, largely based on vendor recommendations.

Q11: Do you prefer a team approach to address this effort, or is a single resource acceptable?
A11: A single resource is acceptable as long as the tests and report can be done timely.

Q12: Is there an incumbent being considered?
A12: No.

Q13: Are there specific security frameworks that the applications need to be assessed against or is it an industry best practices assessment?
A13: Industry best practices assessment.